PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 157134-8 DK	**FOR FURTHER ACTION**	See Form PCT/IPEA/416
International application No. PCT/IL2005/000027	International filing date *(day/month/year)* 09.01.2005	Priority date *(day/month/year)* 07.01.2004
International Patent Classification (IPC) or national classification and IPC INV. H04L12/26 H04L12/24 G06F11/34		
Applicant INTELLINX LTD. et al.		

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 6 sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:
   a. ☒ *sent to the applicant and to the International Bureau)* a total of 13 sheets, as follows:
      ☒ sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).
      ☐ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.
   b. ☐ *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s)) , containing a sequence listing and/or tables related thereto, in celectronic form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).

4. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

Date of submission of the demand	Date of completion of this report
07.11.2005	24.04.2006
Name and mailing address of the international preliminary examining authority: European Patent Office - Gitschiner Str. 103 D-10958 Berlin Tel. +49 30 25901 - 0 Fax: +49 30 25901 - 840	Authorized officer Siebel, C Telephone No. +49 30 25901-485

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/IL2005/000027

Box No. I Basis of the report

1. With regard to the **language**, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.

   ☐ This report is based on translations from the original language into the following language , which is the language of a translation furnished for the purposes of:
   - ☐ international search (under Rules 12.3 and 23.1(b))
   - ☐ publication of the international application (under Rule 12.4)
   - ☐ international preliminary examination (under Rules 55.2 and/or 55.3)

2. With regard to the **elements*** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

Description, Pages

1, 3, 7-23, 26-34	as originally filed
2, 3a, 4, 4a, 5, 6, 24, 25	filed with telefax on 03.04.2006

Claims, Numbers

1-34	filed with telefax on 03.04.2006

Drawings, Sheets

1/12-12/12	as originally filed

☐ a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing

3. ☐ The amendments have resulted in the cancellation of:
   - ☐ the description, pages
   - ☐ the claims, Nos.
   - ☐ the drawings, sheets/figs
   - ☐ the sequence listing *(specify)*:
   - ☐ any table(s) related to sequence listing *(specify)*:

4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).
   - ☐ the description, pages
   - ☐ the claims, Nos.
   - ☐ the drawings, sheets/figs
   - ☐ the sequence listing *(specify)*:
   - ☐ any table(s) related to sequence listing *(specify)*:

* *If item 4 applies, some or all of these sheets may be marked "superseded."*

Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-34
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-34
Industrial applicability (IA)	Yes:	Claims	1-34
	No:	Claims	

2. Citations and explanations (Rule 70.7):

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

The following documents (D) are referred to in this communication; the numbering will be adhered to in the rest of the procedure:

D1: US 6 651 099✓
D2: US 2003/ 0 135 612✓

1. The document D2 is regarded as being the closest prior art to the subject-matter of claim 1 and discloses (the references in parentheses applying to this document):

An apparatus for monitoring and auditing activity in a network, the network utilizes a protocol (i.e. **A:** network recording and filtering of packets: see D2, [4, 36-39, 59], fig. 1a, 1b; **B:** session reconstruction: see D2, [189-192]; Network type: WAN, Internet D2 [002]), the apparatus comprising:

- an analyser operative to analyse intercepted packets conveyed by entities in a network (D2, fig. 15, "packet interpreter", see also fig. 21, [59], [201]) and to generate analysed data based on information associated with at least some of said packets, the analysed data being indicative of sessions (D2, fig. 15, 21, 23, [59], [189-192, 201]; i.e. the analyser is able to filter out packets belonging to a session, see fig. 19); and

- a mirror manager responsive to said analysed data for generating data representative of mirror sessions, each mirror session corresponding to one of said sessions (D2, fig. 15: "multipacket recompiler", "master list"; fig. 19, 21, 23, [189-191, 210]; i.e. all the data concerning a session to be simulated (fig. 23, [189-192])).

- an audit event analyzer (the simulation engine, fig. 23) for processing at least part of said data representative of a mirror session (D2, [197-201], see also [190-193]) and generating data representative of audit events (i.e. eg the data send to the customized web browser, D2, [202]) that include inbound audit events and outbound audit events (implicit: requests for new pages, inputs within web pages, new web pages. etc, seeD2, [197-202]), said outbound audit events including information for instructing a terminal how to draw screens to be displayed thereon (implicit disclosure: web page includes codes for positionning eg. graphical elements, input fields etc.) and serving to prompt a user

to perform operations each, in respect of a corresponding outbound audit event (implicit disclosure: eg input of a password needed during mail access through a web browser), and

said inbound audit events including information representative of the operations performed on the terminal in respect of said outbound audit events (implicit disclosure: the password typed),

1.2 The subject-matter of claim 1 differs in that the apparatus is monitoring a network utilizing an **incremental** protocol and that said audit event analyzer further processing successive one or more outbound audit events and one or more inbound audit events for inscrementally generating cumulative data representative of a respective united audit event that combines preceding outbound and inbound audit events,
said united audit event including information that enables displaying a current status of the screen on a terminal without requiring that the preceding outbound and inbound events be displayed prior thereto.

The subject-matter of claim 1 is therefore new (Article 33(2) PCT).

1.3 The problem to be solved by the present invention may therefore be regarded as how to enable, in an environment **utilizing an incremental protocol,** a displaying of a current status of the screen on a terminal without requiring that the preceding outbound and inbound events be displayed prior thereto.

1.4 The solution proposed in claim 1 of the present application cannot be considered as involving an inventive step (Article 33(3) PCT) for the following reasons:

Incremental protocols are known, eg. X11 traffic, older mainframe-terminal communication protocols and application software. Even todays web formulars are known to be used in such a way, eg: having a page where the user must input data (name, address, account id, passwords). The page might however partly change after an erroneous or missing input of the user and re-become the same (i.e. the input of the user being left in the input fields) after correction of the errors.

In case of that a person skilled in the art is confronted to the problem stated above, it is straightforward for him to either foresee something like setting breakpoints in the script containing the whole transaction (before, during or after a scene being part of the transaction takes/took place) combined with a "play" function to replay the whole script

very quickly until the breakpoints are reached (like eg. in debuggers) OR to define "scenes", (as above, i.e. a transaction between host/terminal being sliced into scenes either before, during or after the scene takes/took place) and treating scenes as an independent bloc. I.e. to view scene X it is not necessary to rebuild the whole transaction beginning from scene 1 until scene X-1, but only to start playing scene X containing a resumé of all important information being necessary to examine scene X. Such a technique is well known eg from books (resumé of the previous book, work, scene, chapter) or eg from MPEG (differential coding), i.e. every Xth frame there is a special frame permitting the terminals to re-synchronize with the current scene. This is eg used if intermediate packets were not correctly received. Another known reason to create such independent blocs is eg related to avoid the need to request big files containing the whole transaction if only part of it is of interest, hence time to retrieve such files is avoided.

2. The method claim 18 contains only features corresponding to the independent appratus claim 1 and is therefore also not inventive (Article 33(3) PCT).

3. Claims 1-17 and 19-34 are dependent on claims 1 and 18 respectively and as such also do not meet the requirements of the PCT with respect to inventive step.

data and the physical address data. The extracted data is then used to access different data bases to determine if matches occur. Time stamps, sequencing and other parameters of each piece of data entering a system are used to control data access.

WO 02/100,039 ("*System and method for traffic management control in a data transmission network*", published 2002) discloses a traffic management system that sniffs data arriving at any point in a system. The sniffer operates to remember certain parameters pertaining to the data. When the amount of data arriving at the point begins to reach a critical level (usually dependent upon data processing capability associated with the point), the system begins to remove (and share) subsequent arriving data based, in part, upon the remembered parameters of recently received data. Data that is stored is returned to the system when the critical threshold recedes.

WO 02/087124 ("*Network analyzer/sniffer with multiple protocol capabilities*", published 2002) discloses systems and methods for automated testing of multiple-protocol network environments wherein data which is formatted according to a plurality of protocols in sequence is automatically identified and compared to determine whether the data has been correctly transformed from each protocol to the next. An indication of whether the data has been correctly transformed may be presented to a user, along with information about the data itself, such as commands which may be included therein. The information presented to the user is in a user-readable form rather than raw data in order to facilitate analysis of the information by the user.

US 6,044,401 ("*Network sniffer for monitoring and reporting network information that is not privileged beyond a user's privilege level*", published 2000) discloses a method and system for locating available information in a network environment by a user in a node. In a system aspect, within a node in the network, the system disclosed in US 6,044,401 includes a network sniffer and an access sniffer. The access sniffer includes an access element and an access interface. The access element preferably includes a memory and a database. The

US 6,651,099 discloses a monitor for and a method of examining packets passing through a connection point on a computer network, each packet conforms to one or more protocols. The method of US 6,651,099 includes receiving a packet from a packet acquisition device and performing one or more parsing/extraction operations on the packet to create a parser record comprising a function of selected portions of the packet. The parsing/extraction operations depend on one or more of the protocols to which the packet conforms. The method of US 6,651,099 further includes looking up a flow-entry database containing flow-entries for previously encountered conversational flows. The lookup uses the selected packet portions and determines if the packet is of an existing flow. If the packet is of an existing flow, US 6,651,099 classifies the packet as belonging to the found existing flow, and if the packet is of a new flow, the method stores a new flow-entry for the new flow in the flow-entry database, including identifying information for future packets to be identified with the new flow-entry. For the packet of an existing flow, the US 6,651,099 updates the flow-entry of the existing flow. Such update may include storing one or more statistical measures. For any stage of a flow, state is maintained, and US 6,651,099 performs any state processing for an identified state to further the process of identifying the flow. US 6,651,099 thus examines each and every packet passing through the connection point in real time until the application program associated with the conversational flow is determined.

US 2003/0135,612 describes systems and methods of full time recording network traffic to a hierarchical data storage. Also described are systems and methods of retrieval of recorded network traffic from a hierarchically organized network data repository. Additionally there are systems and methods of efficiently filtering data in a hierarchically organized network data repository. Systems and methods of displaying recorded network data utilizing the retrieval systems are also included in US 2003/0135,612. Further included are systems and methods of providing sliding time window selection user interfaces.

SUMMARY OF THE INVENTION

By a certain aspect the invention provides an apparatus (**107**) for monitoring and auditing activity of a legacy environment, the apparatus comprising:

an analyzer (303) operative to analyze intercepted packets conveyed by entities (102, 103) in a network and to generate analyzed data based on information associated with at least some of said packets, the analyzed data being indicative of sessions;

a mirror manager (**305**) responsive to said analyzed data for generating data representative of mirror sessions, each mirror session corresponding to a session; and

an audit event analyzer (**307**) for processing at least part of said data representative of mirror sessions and generating data representative of audit events, that include inbound audit events and outbound audit events, said outbound audit events including information representative of screens to be displayed on a terminal; and said inbound audit events including information representative of operations performed on a terminal.

Yet another aspect of the invention is to provide a method for monitoring and auditing activity of a legacy environment, the method comprising:

analyzing (**202**) intercepted packets conveyed by entities in a network;

generating (**203**) analyzed data based on information associated with at least some of said packets, the analyzed data being indicative of sessions;

responsive to said analyzed data generating (204) in respect of each one of one or more of said sessions data representative of a mirror session, each mirror session corresponds to a session; and

processing at least part of said data representative of mirror sessions and generating (206) data representative of audit events that include inbound audit events and outbound audit events; said outbound audit events including information representative of screens displayable on a terminal; and said inbound audit events including information representative of operations performed on a terminal.

By another aspect the invention provides an apparatus for monitoring and auditing activity of legacy environments, the apparatus comprising:

an analyzer server operative to analyze headers of intercepted packets in a session and to generate analyzed packets based on information associated with said headers;

a mirror manager responsive to said analyzed packets for generating mirror sessions;

an audit event analyzer for processing said mirror sessions and generating audit events; and

a business event analyzer for processing said mirror sessions and said audit events and generating business events.

According to certain embodiments the latter apparatus further comprising:

a long term storage memory for archiving said analyzed packets.

BRIEF DESCRIPTION OF THE DRAWINGS

In order to understand the invention and to see how it may be carried out in practice, a preferred embodiment will now be described, by way of non-limiting example only, with reference to the accompanying drawings, in which:

Fig. 1 is a block diagram illustrating a legacy environment that includes an apparatus for monitoring and auditing activity thereof, according to one embodiment of the invention;

Fig. 2 is a flowchart illustrating the main procedures performed by an apparatus for monitoring and auditing activity in a legacy environment, according to one embodiment of the invention;

Fig. 3 is a block diagram illustrating an apparatus for monitoring and auditing activity in a legacy environment, according to one embodiment of the invention;

Fig. 4 is a flowchart illustrating in detail how intercepted packets are analyzed, according to one embodiment of the invention;

Fig. 5 is a flowchart illustrating in detail generation of data representative of mirror sessions, according to one embodiment of the invention;

Fig. 6A illustrates an exemplary screen displayed on a terminal of a clerk in a bank, when opening a new bank account;

Fig. 6B illustrates the same screen of Fig. **6A**, where the input fields include information;

Fig. 6C illustrates at least part of the data representative of the outbound audit event of Fig. **6A**.

Fig. 6D illustrates at least part of the data representative of the inbound audit event including data illustrated in **Fig. 6B**.

Fig. 6E illustrates at least part of the data representative of the united audit event of **Fig. 6B**.

Fig. 7 is a flowchart illustrating in detail generation of data representative of audit events, according to one embodiment of the invention;

Fig. 8 is a flowchart illustrating in detail association of an outbound audit event with an inbound audit event, according to one embodiment of the invention;

Fig. 9 is a flowchart illustrating how a business event is defined, according to one embodiment of the invention; and

Fig. 10 is a flowchart illustrating in detail generation of data representative of business events, according to one embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

In the following description components that are common to more than one figure will be referenced by the same reference numerals.

Fig. 1 is a block diagram illustrating a legacy system **101** that includes an apparatus for monitoring and auditing activity thereof, according to one embodiment of the invention. The legacy system **101** includes entities such as terminals **102** and hosts **103**. For those versed in the art it is realized that terminals **102** usually operate in the legacy systems as clients, while hosts **103** operate as servers. This is non-limiting and alternative or additional entities can also be included in the legacy system. For example, the legacy system **101** includes also printers **104**.

The system includes also at least one sniffer **105** that intercepts network traffic (i.e., packets) conveyed by the entities in the network. The sniffer **105** can connect to the network by any applicable mean, such as connecting to a mirror port of a network switch **106** as illustrated in the figure. It should be appreciated that each sniffer **105** can be pre-configured to intercept network packets conveyed by or to one certain host **103** in the legacy system **101**. In a different

Fig. 6C illustrates at least part **6C01** of the data representative of the outbound audit event of displaying the new customer information screen of Fig. **6A**. In the figure, 01 means "change screen", "C3" stands for UNLOCK **KEYBOARD** and Every occurrence of "11 xx yy" means that the position of the field is calculated based on xx and yy. For example, 11 40 40 means position row 1 column 1 on the screen. Every occurrence of "1d zz" means a new field in this location and its attributes described by zz. The rest are instructions for how to draw the screen. The right side contains a translation from hex to visible characters.

Fig. 6D illustrates at least part **6D01** of the data representative of the inbound audit event including data illustrated in **Fig. 6B**. This part represents the data inserted by the user, i.e., Customer Name: John Doe; Customer ID: 123456 ; and Customer Address: TRUMPET 22 BANFF. In this example, "7D" means "Enter"; "C6 7B" is the cursor position; and the rest are instructions to put specific data representative of part of the screen in specific locations.

Finally, Fig. **6E** illustrates at least part **6E01** of the data representative of the united audit of **Fig. 6B**. It should be appreciated that **6E01** is similar to **6C01**, but include the data of **6D01**.

As long as the user does not logout of the system, allowing another user to login, it is possible to deduce that the logged-in user is associated with the terminal. Therefore, it is possible to include an indication to that user (such as user name or user id) in the data representative of the audit events.

However, in those cases when the mirror session does not start with a connect session (see, for example, **513**, **504** and **505** in **Fig. 5**), the first audit event can be different than the predetermined connection screen. In this case the legacy auditor may not be able to associate a user indication with the data representative of the first and possibly also the coming audit events.

It should be noted though, that the predetermined connection screen can be used in additional opportunities apart from the beginning of a session. In the example that the predetermined connection screen is a login screen it is known

by those versed in the art that a user can logout in the middle of a session, allowing a different user to loin.

Fig. 7 is a flowchart illustrating in detail generation of data representative of audit events, according to one embodiment of the invention. The generation of data representative of audit events occur, for example, in the audit events analyzer **307**. In **701** data representative of a mirror session is received. It is appreciated that the data representative of a mirror session consists at least of analyzed data including intercepted packets, i.e., data representative of a mirror session is also representative of intercepted packets, all the intercepted packets correspond to the same session. Thus, when receiving data representative of a mirror session, the audit events analyzer actually receives data representative of intercepted packets, receiving them in the same order by which they were conveyed to/form the host and terminal.

In **702** the audit events analyzer checks whether the intercepted packet is an outbound or an inbound packet. As was previously explained, outbound packets correspond to a screen conveyed by the host, to be displayed on the terminal, while inbound packets correspond to data conveyed by terminal to the host.

If in **702** the packet is determined to be an outbound packet, the packet belongs to an outbound audit event. Yet, the intercepted packet can indicate that the audit event has just started, or alternatively it can be an in-audit-event packet. In order to determine which of the two alternatives corresponds to the intercepted packet, the audit events analyzer keeps a status variable that indicates whether currently the status is outbound or inbound. If in **703** it is found that the current state is other than outbound, that means that the currently analyzed outbound packet starts a new outbound audit event. Therefore, in **704** the current state is set to be outbound and in **705** a new audit event is initialized for storing data representative of the audit event. For example, a new file is opened and/or a table in a database is initialized etc. The file can include data representative of intercepted packets, together with additional data such as an indication of the

CLAIMS:

1. An apparatus (107) for monitoring and auditing activity in a network, the network utilizes an incremental protocol, the apparatus comprising:

an analyzer (303) operative to analyze intercepted packets conveyed by entities (102, 103, 104) in a network and to generate analyzed data based on information associated with at least some of said packets, the analyzed data being indicative of sessions;

a mirror manager (305) responsive to said analyzed data for generating data representative of mirror sessions, each mirror session corresponding to one of said sessions;

an audit event analyzer (307) for processing at least part of said data representative of a mirror session and generating data representative of audit events that include inbound audit events and outbound audit events, said outbound audit events including information for instructing a terminal how to draw screens to be displayed thereon and serving to prompt a user to perform operations each in respect of a corresponding outbound audit event, and said inbound audit events including information representative of the operations performed on the terminal in respect of said outbound audit events, said audit event analyzer further processing successive one or more outbound audit events and one or more inbound audit events for incrementally generating cumulative data representative of a respective united audit event that combines preceding outbound and inbound audit events, said united audit event including information that enables displaying a current status of the screen on a terminal without requiring that the preceding outbound and inbound events be displayed prior thereto.

2. The apparatus of Claim 1, wherein the analyzer is operative to analyze headers and contents of said intercepted packets.

3. The apparatus of Claim 1, further comprising:

a business event analyzer for processing at least part of said data representative of outbound, inbound and united audit events and generating data representative of business events.

4. The apparatus of Claim 3, further comprising:

an alerts manager (312) coupled to the business event analyzer and being responsive to said data representative of business events for generating alerts.

5. The apparatus of Claim 4, wherein the alerts manager generates at least some of the alerts based on predetermined thresholds.

6. The apparatus of any one of the preceding claims, wherein said entities include hosts (103) and terminals (102).

7. The apparatus of any one of the preceding claims further comprising:

a first long term storage device (304) for storing at least part of said analyzed data.

8. The apparatus of any one of the preceding claims further comprising:

a second long term storage device (306) for storing at least part of said data representative of mirror sessions.

9. The apparatus of any one of Claims 1 to 7, further comprising:

a compression agent (313) for compressing at least part of the data representative of mirror sessions.

10. The apparatus of claim 8, further comprising:

a compression agent (313) for compressing at least part of the data representative of mirror sessions.

11. The apparatus of Claim 10, wherein the compression agent (313) is configured to compress the data representative of mirror sessions before the second long term storage device stores the at least part of the data representative of mirror sessions.

12. The apparatus of any one of Claims 1 to 7 and 9, further comprising:

an encryption agent (314) for encrypting at least part of the data representative of mirror sessions.

13. The apparatus of any one of Claims 8, 10 and 11, further comprising:

an encryption agent (314) for encrypting at least part of the data representative of mirror sessions.

14. The apparatus of Claim 13, wherein the encryption agent (314) is configured to encrypt the data representative of mirror sessions before the second long term storage device stores the at least part of the data representative of mirror sessions.

15. The apparatus of any one of Claims 1 to 7, 9 and 12, further comprising:

a signature agent (315) for digitally signing at least part of the data representative of mirror sessions.

16. The apparatus of any one of Claims 8, 10, 11, 13 and 14, further comprising:

a signature agent (315) for digitally signing at least part of the data representative of mirror sessions.

17. The apparatus of Claim 16, wherein the signature agent (315) is configured to sign the data representative of mirror sessions before the second long term storage device stores the at least part of the data representative of mirror sessions.

18. A method for monitoring and auditing activity in a network, the network utilizes an incremental protocol, the method comprising:

analyzing intercepted packets conveyed by entities in a network;

generating analyzed data based on information associated with at least some of said packets, the analyzed data being indicative of sessions;

responsive to said analyzed data generating in respect of one or more of said sessions data representative of one or more mirror sessions, each mirror session corresponding to a session; and

processing at least part of said data representative of a mirror session and generating data representative of audit events that include inbound audit events and outbound audit events, said outbound audit events including information for instructing a terminal how to draw screens to be displayed thereon and serving to prompt a user to perform operations each in respect of a corresponding outbound audit event, and said inbound audit events including information representative of the operations performed on the terminal in respect of said outbound audit events, wherein processing further includes processing successive one or more outbound audit events and one or more inbound audit events for incrementally generating cumulative data representative of a respective united audit event that combines preceding outbound and inbound audit events, said united audit event including information that enables displaying a current status of the screen on a terminal without requiring that the preceding outbound and inbound events be displayed prior thereto.

19. The method of Claim 18, wherein analyzing intercepted packets includes analyzing headers and contents of said packets.

20. The method of Claim 18, further comprising:

processing at least part of said data representative of outbound, inbound and united audit events and generating data representative of business events.

21. The method of Claim 20, further comprising:

responsive to said data representative of business events generating alerts in respect of at least one of said business events.

22. The method of Claim 21, wherein generating at least some of the alerts is based on predetermined thresholds.

23. The method of any one of Claims 18 to 22, further comprising:

storing at least part of the analyzed data.

24. The method of any one of Claims 18 to 23, further comprising:

storing at least part of the data representative of mirror sessions.

25. The method of Claims 18 to 23, further comprising:

compressing at least part of said data representative of mirror sessions.

26. The method of Claim 24, further comprising:

compressing at least part of said data representative of mirror sessions.

27. The method of Claim 26, wherein compressing the at least part of said data representative of mirror sessions is performed before storing the at least part of the data representative of mirror sessions.

28. The method of any one of Claims 18 to 23 and 25, further comprising:

encrypting at least part of said data representative of mirror sessions.

29. The method of any one of Claims 24, 26 and 27, further comprising:

encrypting at least part of said data representative of mirror sessions.

30. The method of Claim 29, wherein the encrypting the at least part of said data representative of mirror sessions is performed before storing the at least part of the data representative of mirror sessions.

31. The method of any one of Claims 18 to 23, 25 and 28 further comprising:

digitally signing at least part of said data representative of mirror sessions.

32. The method of any one of Claims 24, 26, 27, 29 and 30 further comprising:

digitally signing at least part of said data representative of mirror sessions.

33. The method of Claim 32, wherein digitally signing the at least part of said data representative of mirror sessions is performed before storing the at least part of the data representative of mirror sessions.

34. The method of claim 18, wherein the united audit event is displayable on a screen.